AFFIDAVIT

I, Colin Simons, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) currently assigned to the Rutland, Vermont Resident Agency of the Albany, New York Division. I have been a Special Agent for over 15 years. I am responsible for working cases involving a variety of criminal violations, to include violent crimes and gangs. I have also been the affiant to numerous federal complaints and search warrants pertaining to violent crime and drugs. As a Special Agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of three electronic devices, described with particularity in Attachment A, which are currently stored in evidence at the Burlington Police Department in Burlington, Vermont, and the extraction from the cellular telephone of electronically stored information described in Attachment B.

3. Based on my training and experience I know the following:

a. Persons who participate in the distribution of controlled substances frequently use cellular phones and other electronic devices to coordinate their unlawful activities, and to maintain contact with suppliers and consumers of illegal drugs.

b. I know that information stored in the memories of these communications devices constitutes evidence of drug trafficking and or the illegal movement of currency. Among other things, the evidence may contain the telephone numbers assigned to the communication devices, messages received by or sent from the devices, identification numbers and other information contained in their electronic memories, and the records of telephone numbers to

which calls were placed and from which calls were received.

c. With their cellular phones, drug traffickers often take photographs of other members of their organizations, assets obtained from profits of drug sales, locations associated with their illegal activity, and other useful evidence.

d. I also know that persons engaged in such illegal activity will often deny ownership of these phones in an attempt to thwart law enforcement's efforts to connect them to more serious crimes, possible co-conspirators, and/or their sources of supply.

e. Data contained in a cell phone may reveal the physical location of the cell phone at various times. For example, the latitude and longitude of the camera at the time it takes a photograph will be contained in the metadata associated with the picture. Also, if a cellular phone has Global Positioning System ("GPS") capabilities (which many do), additional information regarding locations of the phone, while it follows GPS directions, may be recovered from the device.

4. The property to be searched is the contents of the following three devices, collectively referred to hereafter as "Electronic Devices," seized on April 11, 2019:

a. Samsung Model SM-B311V, with MEID HEX: A00000476E68BC

b. Samsung Model SM-B311V, with MEID HEX: A0000048D82A89

c. Apple iPhone with black "Speck"-brand case.

The applied-for warrant would authorize the forensic examination of the Electronic Devices listed above, for the purpose of identifying electronically stored data particularly described in Attachment B.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that evidence of crimes committed by Curtis Bunkley and others, namely possession with intent to distribute and

distribution of controlled substances, in violation of 21 U.S.C. §§ 841(a)(1) and 846, is located in the Electronic Devices. The Electronic Devices are currently stored in evidence in a secure vault at the Vermont State Police Barracks in Westminster, Vermont.

6. I am familiar with the facts and circumstances of this investigation from: (a) my own personal involvement in the investigation and my personal observations; (b) reports and affidavits made available to me by other law enforcement authorities, and (c) my discussions with the foregoing individuals and other law enforcement officers. Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not set forth each and every fact learned by law enforcement during the course of the investigation.

PROBABLE CAUSE

7. On April 9, 2019, the Honorable John M. Conroy, United States Magistrate Judge for the District of Vermont, issued an arrest warrant for Curtis Bunkley, having found probable cause to believe that Bunkley distributed cocaine base on April 3, 2018, and heroin on January 14, 2019. A copy of the Criminal Complaint and supporting Affidavit are attached as Exhibit 1, and incorporated herein by reference. Exhibit 1 remains true and correct.

8. On April 11, 2019, Vermont State Police Detective Andrew Todd was conducting surveillance at the known residence of Bunkley, 134 Morningside Commons, Brattleboro, Vermont, and observed Bunkley depart the area at approximately 9:00 am. At approximately 11:38 am, Vermont State Police Trooper Zachary VanValkenburgh observed a silver Dodge Durango approach Bunkley cms ~~his~~ residence at 134 Morningside Commons, Brattleboro, Vermont. Trooper VanValkenburgh observed the Durango exceeding the posted speed limit, and conducted a traffic stop of the vehicle. Bunkley, who was driving and the sole occupant of the vehicle, was ordered out of the Durango. A search of Bunkley incident to his arrest resulted in the seizure of approximately 300 glassine baggies

of suspected heroin from a pocket of Bunkley's pants. Trooper VanValkenburgh also located a receipt on Bunkley's person; the receipt was from the McDonalds in Greenfield, Massachusetts showing a purchase occurring at approximately 9:28 am on April 11, 2019. Bunkley was transported to the Vermont State Police barracks in Westminster, Vermont for processing and interviewing.

9. Bunkley waived his Miranda rights, and agreed to answer questions. I participated in the interview of Bunkley. This account of the interview is not meant to be a verbatim account, but rather a summary of information that Bunkley provided. During questioning, Bunkley made general admissions to having distributed heroin in the Brattleboro area, mentioning specific customers by name, and admitted to having traveled to the area of Turners Falls, Massachusetts earlier on April 11, 2019 for a haircut.

10. Based on my training and experience, I know that Greenfield, Massachusetts is a "source city" for narcotics, in that drug distributors and drug addicts frequently travel to Greenfield, Massachusetts for the purpose of purchasing heroin and cocaine base, which they bring back to Vermont for distribution and use.

11. Laboratory testing of 10 of the 300 seized bags of suspected heroin revealed that each of the 10 bags contained controlled substances. Some of the bags were a mixture of heroin and fentanyl. Other bags contained a mixture of heroin, fentanyl, and acetyl fentanyl. Based on my training and experience, I know 300 baggies of heroin to be significantly in excess of a personal-use quantity.

12. A search of Bunkley's Dodge Durango after Bunkley's arrest resulted in the seizure of three cellular telephones (the Electronic Devices):

a. **Samsung Model SM-B311V, with MEID HEX: A00000476E68BC**

b. **Samsung Model SM-B311V, with MEID HEX: A0000048D82A89**

c. Apple iPhone with black "Speck"-brand case.

The Electronic Devices have been stored in evidence at the Vermont State Police Barracks in Westminster, Vermont, since their seizure, and I believe the contents of the Electronic Devices to be the same as at the time of seizure.

13. Based on my knowledge and experience and direct participation in investigations into the distribution of controlled substances, including heroin, fentanyl, and cocaine base, I know that:

(a) Distribution of controlled substances can be lucrative, and individuals who engage in such conduct are capable of amassing tens of thousands of dollars or more in a short period of time and often physically retain such currency for long periods of time, even after their distribution activity has ceased;

(b) It is common for sellers of controlled substances to put bank accounts, assets, and cell phones in the names of associates or fictitious names to avoid detection and to conceal illegitimate income;

(c) Controlled substance traffickers maintain and access books, records, receipts, bills of sale, notes, ledgers, computer software, airline tickets, money orders, and other documents relating to the transportation, acquisition, and distribution of controlled substances and proceeds, and much of this information is commonly stored electronically in Electronic Devices and other electronic devices capable of storing electronic data;

(d) Traffickers in controlled substances commonly maintain names and contact information in books, ledgers, telephones, computers, personal digital assistants (PDAs), Electronic Devices and other digital Devices, and digital storage media, which reflect the names addresses, telephone numbers, and email addresses of their drug trafficking associates;

(e) Persons involved in large scale drug trafficking keep and access electronic records of the storage, purchase, and/or trading in large amounts of currency, financial instruments (including stocks, bonds, certificates of deposit, etc.), precious metals, jewelry, automobile titles, other items of value and/or proceeds of drug transactions and evidence of financial transactions relating to the attainment and concealment of large sums of money, i.e. bank statements, check registers, financial account statements, wire transfer records and documentation of foreign bank accounts, acquired from engaging in narcotic trafficking

activities; these items are often stored inside their Electronic Devices long after they cease trafficking in drugs;

(f) When drug traffickers amass proceeds from the sale of drugs, the drug traffickers attempt to legitimize these profits, i.e., "launder" the profits. To accomplish these goals, drug traffickers many times utilize domestic and foreign banks and/or financial institutions with their attendant services, including sales of securities, cashier checks, money drafts, money orders, letters of credit, etc. Other entities used to "launder" monies include brokerage houses, real estate firms, shell corporations and purported legitimate business fronts. Electronically stored evidence of their attempts to legitimize or "launder" the proceeds is commonly secreted within the electronic storage of their Electronic Devices long after they cease trafficking drugs;

(g) Persons engaged in criminal activity often spend the proceeds of their criminal activity and maintain or access records of their expenditures on their Electronic Devices, long after their criminal activity has ceased. They also maintain electronic records reflecting communication with their criminal associates. Specifically, these records may include the following;

i. Records of income and expenses, such as profit and loss statements and income and expense journals that reflect the expenditure of the proceeds of criminal activity;

ii. Evidence of the expenditure of the proceeds of criminal activity or purchase of assets with the proceeds of criminal activity, such as invoices, receipts, rental statements, lease statements, travel records, earnest money agreements, escrow statements, and real estate deeds:

iii. Records of the accumulation of assets acquired with the proceeds of criminal activity, such as ledgers, balance sheets and financial statements, reflecting both assets and liabilities;

iv. Checking and savings account records consisting of monthly statements, duplicate deposit slips, and canceled checks reflecting the deposit and disbursement of the proceeds of criminal activity;

v. Letters and other documents reflecting communications between partners or associates, such as address and phone books reflecting the names and addresses of partners or associates, phone billing records reflecting telephone activity, contracts and other

agreements reflecting associations between individuals relative to business ventures, and cashier's checks, money orders, and wire transfers that are evidence of transactions involving the proceeds of criminal activity;

vi. Drug traffickers frequently take or cause to be taken, photographs of themselves, their associates, their property, and their product. These traffickers usually maintain these photographs electronically in their Electronic Devices. I know, based on my training and experience, that federal courts have recognized that unexplained wealth is probative evidence of crimes including trafficking in controlled substances.

14. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Cellular telephone: A cellular telephone (or mobile telephone, or wireless telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A cellular telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, Electronic Devices offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Electronic Devices may also include global positioning system ("GPS") technology for determining the location of the device.

b. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication Devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs

run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device. PDAs also often contain digital cameras.

c. Smart Phone: Smart phone is a term typically used to refer to a cellular telephone that has combined the capabilities of a typical cellular telephone and a typical PDA.

d. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

e. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation Devices can give a user driving or walking directions to another location. These Devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent

from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic Devices that communicate with each other. Due to the structure of the Internet, connections between Devices on the Internet often cross state and international borders, even when the Devices communicating with each other are in the same state.

15. Based on my training and experience, I know the Apple iPhone listed in Attachment A to be a Smart Phone, and include the features outlined above. Based on my review of the user manual for the Samsung Model SM-B311V, I know this model of cellular phone to have a digital camera, GPS technology, the ability to send text/photo messages, limited email capabilities, and rudimentary internet-browsing functions.

16. In addition, I submit that there is probable cause to believe records may be stored on the Electronic Devices for at least the following reasons:

a. Based on my knowledge, training, experience and discussions with other law enforcement officers, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer or smart phone, the data contained in the file does not actually disappear; rather, that data remains on the device's storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the storage medium that is not currently being used by an active file – for long periods of time before they are overwritten. In addition, a device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media – in particular, a device's internal hard drives – contain electronic evidence of how a computer has been used, what it has been used for, and who has used it (user attribution). To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

17. As further described in Attachment B, this application seeks permission to locate not only digital files that might serve as direct evidence of the crimes described in the warrant, but also for forensic electronic evidence that establishes how the device was used, the purpose of their use, who used them, and when. There is probable cause to believe this forensic electronic evidence will be on the Electronic Devices for the following reasons:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage Devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created, and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and

prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus spyware and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a cellular telephone works can, after examining this forensic evidence in its proper context, draw conclusions about how a cellular telephone was used, the purpose of its use, who used it, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a cellular telephone was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

18. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

19. Based on the foregoing, I submit probable cause exists to search the Electronic Devices, more specifically described in Attachment A, for the evidence delineated in Attachment B.

Colin Simons
Special Agent, FBI

Sworn to and subscribed before me this 13th day of September, 2019.

John M. Conroy
United States Magistrate Judge